فصلنامه علمی مطالعات بین‌رشته‌ای دانش‌راهبردی
سال دوازدهم، شماره ۴۸، پاییز ۱۴۰۱، صفحه ۸۹-۶۵

مقاله پژوهشی: ارائه مدل مفهومی آمادگی رزم سایبری نیروهای مسلح ج.ا.ا

20.1001.1.24234621.1401.12.48.3.7

حسن محمدی منفرد[۱]

تاریخ دریافت: ۴ / ۳ /۱۴۰۰ **تاریخ پذیرش: ۱۴۰۰/۵/۱۰**

چکیده

برنامه‌ریزی برای حفظ و افزایش میزان آمادگی رزم سایبری، به واسطه نقش با اهمیت آن در افزایش قدرت بازدارندگی جمهوری اسلامی ایران، ضرورت قطعی و گریز ناپذیر نیروهای مسلح می‌باشد. پژوهش حاضر با هدف شناسایی ابعاد و معیارهای الزامی و موثر در آمادگی رزم سایبری انجام شد. لذا این پژوهش، از نظر هدف کاربردی و از حیث گردآوری داده‌ها، توصیفی- پیمایشی محسوب می‌شود. روش این پژوهش کیفی- کمی(آمیخته) و جامعه آماری آن شامل خبرگان در رابطه با موضوع این تحقیق است که می‌توان از اساتید دانشگاهی، مدیران و کارشناسان حرفه ای در سطوح ستادی و عملیاتی نام برد؛ در مرحله نمونه گیری به منظور انجام مصاحبه و نظرخواهی، از روش گلوله برفی استفاده شد. در بخش کیفی تعداد ۱۰ مصاحبه موفق ثبت گردید. همچنین در بخش کمی تعداد۳۰ نفر از جامعه آماری مورد اشاره برای پاسخ به پرسشنامه محقق‌ساخته انتخاب گردیدند. برای تجزیه و تحلیل یافته ها، از روش کدگذاری داده ها و روش های آماری ناپارامتریک بهره‌گیری شد. آلفای کرونباخ محاسبه شده در نرم افزارSPSS برای دو بخش ابعاد، و اولویت بندی در نظر گرفته شده در پرسشنامه، به ترتیب ۰/۸۱ و ۰/۸۹ می‌باشد که نشانگر پایایی خوب و قابل قبولی است. مطابق یافته‌های تحقیق، الگوی مفهومی آمادگی رزم سایبری در قالب ۱۷ مؤلفه و ۴ بعد شامل: بستر رزم‌سایبری، بازیگران عملیاتی، روش رزم‌سایبری و و نهایتا نحوه فرماندهی، مدیریت و هدایت سایبری، تدوین و ارائه شده است

کلیدواژه‌ها: الگو، رزم سایبری، نیروهای مسلح. آمادگی رزم سایبری

[۱] . دانش آموخته مدیریت راهبردی فضای سایبر دانشگاه عالی دفاع ملی (نویسنده مسئول) h.mohammadi@sndu.ac.ir

مقدمه

آمادگی برای جنگ وظیفه‌ای است که خداوند متعال درآیه شریفه« *وَأَعِدّوا لَهُم مَا استَطَعتُم مِن قُوَّةٍ وَمِن رِباطِ الخَیلِ تُرهِبونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّکُم*[1] به طور صریح بر عهده مسلمانان گذاشته است. امام خامنه ای(مدضله العالی) در دیدار جمعی از فرماندهان و کارکنان ارتش جمهوری اسلامی ایران در تاریخ ۱۳۹۴/۰۱/۳۰ می‌فرمایند: «همهٔ دستگاه‌های جمهوری اسلامی ایران از وزارت دفاع تا سازمان‌های ارتش و سپاه و دیگر دستگاه های مختلف، باید آمادگی‌ها را روزبه روز افزایش بدهند؛ هم در زمینهٔ تسلیحات، هم در زمینهٔ سازماندهی‌ها، هم در زمینه آن چیزی که در نیروهای مسلّح بیشترین تأثیر را دارد. حفظ بصیرت، حفظ جهت‌گیری صحیح، روحیهٔ خوب و افزایش روز افزون تجهیزات و امکانات یکی ازکارهای اساسی‌ای است که نیروهای مسلّح بایستی داشته باشند». همچنین در سیاست‌های کلی نظام نیز به طورخاص به ارتقای آمادگی نیروهای مسلح برای بازدارندگی و مقابله موثر در برابر تهدیدها، حفاظت از منافع ملی و انقلاب اسلامی اشاره شده است.اما نکته قابل‌توجه در آمادگی‌رزمی، چگونگی آمادگی نیروهای مسلح در برابر تهدیدات نوین از جمله تهدیدات سایبری می‌باشد. چراکه امروزه یکی از بهترین و کم هزینه‌ترین روش‌ها و گزینه‌های حمله به دیگر کشورها، بهره‌برداری از ویژگی‌ها و ظرفیت‌های فضای سایبری است.

متاسفانه فضای سایبر به واسطه نو پدید بودن و نگاه توسعه‌ای به آن از یک طرف، و پیچیدگی شرایط و ویژگی‌های فضای سایبر از طرف دیگر، بخش دفاعی- امنیتی کشور را با طیف وسیع و پیچیده‌ای از تهدیدات سایبری، فراوانی متغیرها، تنوع و تعدد بازیگران بین‌المللی و منطقه‌ای، افزایش ماموریت‌ها و وظایف رزمی و فشارهای مالی و بودجه‌ای مواجه نموده و این چالش‌ها در آینده نیز بیشتر خواهد شد. در نتیجه فهم و جهت‌گیری سیستمی در ارتباط با نهادینه کردن، مولفه‌های آمادگی رزم سایبری یک ضرورت و مساله اساسی محسوب می‌گردد. لذا ارائه الگوی مفهومی آمادگی رزم سایبری به منظور زمینه‌سازی و ایجاد ساز و کار و چارچوب هایی برای انجام تکالیف فردی و سازمانی و هم افزایی بین آن ها به گونه‌ای که نیروهای مسلح جمهوری اسلامی

[1] . سوره مبارکه الأنفال آیه ۶۰

ایران قادر به افزایش میزان آمادگی رزم سایبری و یا حفظ آن، به واسطه نقش با اهمیت آن در افزایش قدرت بازدارندگی جمهوری اسلامی ایران باشند، ضرورت قطعی و گریز ناپذیر نیروهای مسلح می‌باشد. با توجه به دغدغه های مطرح‌شده بالا و با عنایت به اینکه تبیین مفهوم آمادگی رزم سایبری را می توان گام نخست برنامه های توسعه این حوزه دانست، هدف و سؤال اصلی این پژوهش، دستیابی به الگوی مفهومی آمادگی رزم سایبری می باشد. لذا سؤالات فرعی زیر پژوهش را در جهت نیل به ترسیم الگوی مفهومی هدایت می نماید.

۱- ابعاد مؤثر در آمادگی رزم سایبری نیروهای مسلح ج.ا.ا کدامند؟

۲- مؤلفه های مؤثر در آمادگی رزم سایبری نیروهای مسلح ج.ا.ا کدامند؟

۳- وضعیت اولویت بندی ابعاد و مؤلفه های این حوزه چگونه است؟

پیشینه شناسی

(۱) مرکز بلفر وابسته به دانشگاه هاروارد آمریکا در سال ۲۰۲۰ میلادی، مدلی را برای اندازه گیری قدرت سایبری ملی کشورها ارائه نموده است. در این مدل بیان شده است که قدرت سایبری از چندین اجزای سازنده تشکیل شده است که بایستی در متن توجه اهداف ملی کشورها قرار گیرد. این الگو برای اندازه‌گیری قدرت سایبری، رویکرد کلان کشور و همه‌ی جوانب تحت کنترل دولت را در نظر گرفته است. در این مدل رتبه بندی کلی یک کشور بر اساس میانگین هفت هدف ملی به شرح زیر است:

- نظارت بر گروه های داخلی
- تقویت و بهبود دفاع سایبری ملی
- کنترل و اداره کردن محیط اطلاعات
- جمع آوری اطلاعات پنهان
- بهبود و افزایش رشد صنایع داخلی
- تخریب یا غیر فعال کردن زیرساخت ها و قابلیت های نیروهای متخاصم
- تعریف هنجارها و استانداردهای بین المللی سایبری

بر اساس این شاخص ها، کشورهای آمریکا، چین، انگلستان، روسیه و هلند، به عنوان ۵ کشور برتر در این رتبه بندی معرفی شدند. همچنین ایران در رتبه ۲۳ قرار گرفت (بلفر،۲۰۲۰).

(۲) مؤسسه مطالعاتی **ABI Research** و اتحادیه بین المللی ارتباطات از راه دور برای اولین بار در سال ۲۰۱۴ پژوهشی را با عنوان تعیین شاخص امنیت سایبری جهانی[1]انجام دادند. که گزارش نتایج آن به صورت سالانه برای دولت ها و سیاستگذاران منتشر می گردد. این طرح، امنیت سایبری کشورها را در پنج بعد شامل: اتخاذ اقدامات قانونی، اقدامات فنی، اقدامات سازمانی، ظرفیت سازی و همکاری در حوزه سایبر با ۱۷ شاخص، به منظور ارائه بینش امنیت سایبری در کشورها انجام شده است. البته هدف اصلی این طرح، توجه دادن دولت ها به گنجاندن مبحث امنیت سایبری در حوزه های مختلف فعالیتشان و شناسایی حوزه های ضعف و قوت آنها در این حوزه می باشد.

(۳) مؤسسه تحقیقات دفاع ملی ایالات متحده آمریکا (۱۹۹۱)، پژوهشی با عنوان « ارتقای نظام اندازه‌گیری آمادگی و پایداری نظامی ایالات متحده آمریکا» با هدف شناسایی مدلی برای اندازه‌گیری و بهبود آمادگی و پایداری نظامی انجام داد. در نهایت این تحقیق به مدلی برای اندازه گیری قابلیت نظامی رسید که دارای چهار مؤلفه اصلی به شرح زیر می باشد:

۱- ساختار نیروی نظامی(تعداد، اندازه و ترکیب واحدها و اجزایی که نیروهای مسلح را شکل می‌دهند).

۲- نوسازی نیروی نظامی (شامل کیفیت فنی نیروها، واحدها، سیستم‌های سلاح و تجهیزات می‌باشد).

۳- آمادگی[2] توانایی نیروها، واحدها، سیستم‌های سلاح و تجهیزات برای انجام ماموریت‌های محوله).

۴- پایداری[3]نیروی نظامی (شامل توان حفظ نیروها، واحدها، سیستم‌های سلاح و تجهیزات).

(۴) هلیلی و همکاران پژوهشی با عنوان« قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی» با هدف مفهوم سازی قدرت سایبری با رویکرد فرکتالی و تأثیر آن بر امنیت ملی انجام دادند. در این پژوهش مفهوم قدرت سایبری در قالب سه بعد؛ سخت، نیمه سخت و نرم و ۱۵ مؤلفه و رابطه میان آن ها تبیین شد. نتایج این تحقیق نشان می‌دهد، داشتن منابع، تجهیزات و فناوریهای سایبری، شرط لازم برای دستیابی به امنیت ملی است(هلیلی و همکاران،۱۳۹۷).

(۵) نصرت آبادی در رساله‌ی دکتری با عنوان «الگوی ارزیابی قدرت سایبری نیروهای مسلح ج.ا.ا» با هدف دستیابی به الگوی راهبردی سنجش قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران با روش

1 . Global Cybersecurity Index
2 .Readiness
3 . Sustainability

آمیخته و اخذ نظر خبرگان و کارشناسان سایبری انجام داد. نتایج این پژوهش، الگوی مذکور را، در قالب سه بعد آفند سایبری، پدافند سایبری، تاب آوری سایبری و یازده مؤلفه و پنجاه وپنج شاخص ارائه گردید.(نصرت آبادی و همکاران،۱۳۹۸).

مفهوم شناسی و مبانی نظری تحقیق

فضای سایبر

طی سال‌های اخیر، تعاریف زیادی برای واژه فضای سایبر ارائه و به مرور تکمیل شده است. در جدول(۱) برخی تعاریف واژه فضای سایبر در اسناد راهبردی سایبری کشورها و مراجع بین المللی استاندارد، ارائه می گردد.

جدول۱: تعریف فضای سایبر در اسناد راهبردی کشورها

ردیف	اسناد راهبردی	تعریف	منبع
۱	**اسناد راهبردی آمریکا**	فضای سایبر، شامل شبکه های وابسته به یکدیگر، از زیرساخت های فناوری اطلاعات، اعم از اینترنت، شبکه های ارتباطی، سامانه های رایانه ای، پردازنده های جاگذاری شده و کنترل کننده های صنایع حیاتی می باشد	(دانشگاه جنگ ارتش آمریکا، ۲۰۱۲) .
۲	**تعریف مشترک روسیه و آمریکا**	فضای سایبر، محیط الکترونیکی است که اطلاعات در آن تولید، ارسال، دریافت، ذخیره سازی، پردازش و حذف می گردد.	(انستیتو شرق-غرب آمریکا و روسیه مسکو،۲۰۱۱).
۳	**سند راهبرد امنیت فضای سایبر انگلیس**	فضای سایبر، یک محیط تعاملی متشکل از شبکه های دیجیتال است که برای ذخیره سازی، اصلاح و مبادله اطلاعات مورد استفاده قرار می گیرد. فضای سایبر، شامل اینترنت و سایر سامانه های اطلاعاتی که زیرساخت، سرویس ها و کسب و کار را پشتیبانی می کنند نیز می شود	**(کابینه انگلیس،۲۰۱۱)**
۴	**اسناد ناتو**	فضای سایبر، فراتر از شبکه اینترنت است و نه تنها شامل سخت افزار، نرم افزار و سامانه های اطلاعاتی، بلکه شامل افراد و تعاملات اجتماعی آنها در داخل این شبکه ها نیز می باشد	**(مرکز مشارکتی نخبگان دفاع سایبری ناتو، ۲۰۱۲)**

ردیف	اسناد راهبردی	تعریف	منبع
۵	**فضای سایبر در اسناد موسسه بین المللی استاندارد**	عبارت است از نتیجه ی تعاملات انسان با شبکه ها و تجهیزات فناورانه متصل به اینترنت که موجودیت فیزیکی ندارند	**(چارچوب امنیت ملی سایبر،۲۰۱۲)**
۶	**اسناد جمهوری اسلامی ایران**	عبارت است از شبکه های وابسته به یکدیگر، از زیرساخت های فناوری اطلاعات، شبکه های ارتباطی، سامانه های رایانه ای، پردازنده های تعبیه شده (جاگذاری شده)، کنترلگرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره برداری از اطلاعات می باشد. این فضا، ممکن است در ارتباط مستقیم و مداوم با سامانه های فناوری اطلاعات و شبکه های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد	**(سند پدافند سایبری، ۱۳۹۴).**

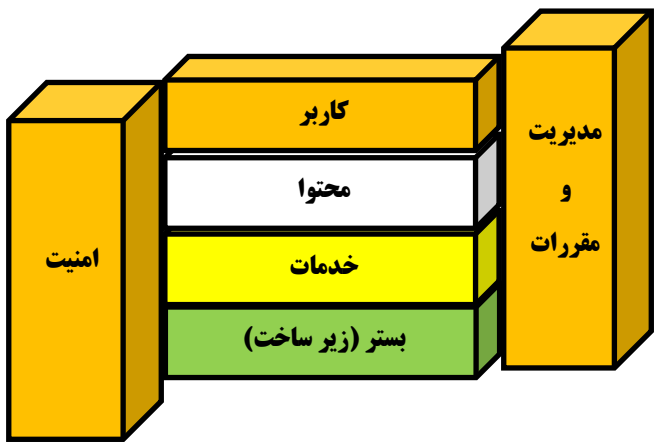
فضای سایبری یک قلمرو جهانی در محیط اطلاعاتی است که از شبکه وابسته به هم از زیرساخت های فناوری اطلاعات شامل اینترنت، شبکه های مخابراتی، سیستم های رایانه ای و پردازشگرها و کنترلرهای جاسازی شده تشکیل شده است(آندرس و وینترفلد[1]،۲۰۱۴). همچنین براساس تعاریف وزارت دفاع آمریکا، محیط اطلاعاتی عبارت است از: «مجموعه ای از افراد، سازمان ها و سیستم هایی که اطلاعات خود و دیگران را جمع آوری، پردازش یا منتشر می کنند یا بر اساس اطلاعات، اقدام می‌کنند. محیط اطلاعاتی یک مجموعه به هم مرتبط از اطلاعات، زیرساخت‌های اطلاعاتی و فرایندهای مبتنی براطلاعات است. یک سیستم اطلاعاتی تلفیقی از حسگرها، شبکه‌ها، پردازشگرها،

1 .Andress &Winterfeld

مراکز فرماندهی و اپراتورها است. بر اساس تعریف فوق و دیگر اسناد منتشر شده آمریکایی‌ها محیط اطلاعاتی دارای ابعاد فیزیکی، اطلاعاتی و شناختی می باشد. البته همانطور که در خصوص محیط اطلاعاتی عنوان شد، فضای سایبر نیز دارای ابعاد فیزیکی، اطلاعاتی و شناختی می‌باشد.

اجزای تشکیل دهنده فضای سایبر

لیبیکی و مارتین در کتاب غلبه بر فضای سایبر، این فضا را مشتمل بر سه لایه ی فیزیکی، نحوی و معنایی می دانند(لیبیکی و مارتین،۲۰۰۷). در طرح قابلیت های مفهومی ارتش آمریکا برای عملیات در فضای سایبر طی سال‌های ۲۰۱۶ تا ۲۰۲۸، فضای سایبر را شامل سه لایه ی فیزیکی، منطقی و اجتماعی تعریف کرده است (فرماندهی آموزش و دکترین،۲۰۱۰). دیوید کلارک در مقاله ای با عنوان «توصیف فضای سایبر: گذشته، حال و آینده» مدل ۴ لایه ای، شامل لایه های فیزیکی، منطقی، اطلاعات و کاربران را برای توصیف فضای سایبر ارائه نموده است (دیوید کلارک، ۲۰۱۰). همچنین از نظر لیور تابانسکی، فضای سایبر از سه لایه‌ی زیر ساخت، منطق نرم‌افزاری و اطلاعات تنظیم شده است (لیور تابانسکی،۲۰۱۱). **در تعریف مشترک روسیه و آمریکا، فضای سایبر به دو بخش زیرساخت سایبری و خدمات سایبری تفکیک شده است (انستیتو شرق-غرب آمریکا و انستیتو امنیت اطلاعات دانشگاه دولتی مسکو،۲۰۱۱).** در مقاله روش شناسی عملیات سایبری در بافتار عملیات نظامی، فضای سایبر به چهار لایه‌ی فیزیکی، منطقی، شخصیت سایبری و نظارت تفکیک شده است (انتشارات مرکز مشارکتی نخبگان دفاع سایبری ناتو،۲۰۱۲). جوزف نای در کتاب آینده ی قدرت فضای سایبر را مشتمل بر دولایه ی زیرساخت فیزیکی واطلاعاتی معرفی نموده است (جوزف نای،۲۰۱۳). شورای عالی فضای مجازی یک مدل چهار لایه ای برای فضای سایبری کشور ارائه داده است که در شکل۱ آمده است.



شکل (۱): مدل چهار لایه ای فضای سایبر (مرکز ملی فضای مجازی، ۱۳۹۶)

لایه زیرساخت: این لایه برای ذخیره سازی، انتقال و پردازش اطلاعات در فضای سایبر مورد استفاده قرار می گیرد.

لایه خدمات: به سرویس ها و یا خدماتی که در فضای سایبر ارائه می گردد، اشاره دارد.

لایه محتوا: به محتوا و اطلاعات ارجاع دارد که در فضای سایبری وجود داشته و ابزارهایی که برای دستیابی و پردازش این اطلاعات مورد استفاده قرار می‌گیرند

لایه کاربر(انسانی/اجتماعی): به ارتباطات و تعامل‌های بین کاربران در فضای سایبر و اطلاعاتی که به اشتراک می‌گذارند اشاره دارد. همچنین هرکدام از این لایه‌های فضای سایبر از اجزایی تشکیل شده اند که در جدول(۲) به آن اشاره شده است.

جدول(۲): اجزای تشکیل دهنده لایه‌های فضای سایبر (تقی پور و دیگران،۱۳۹۸)

ردیف	عنوان لایه	اجزاء تشکیل دهنده لایه
۱	**زیر ساخت**	زیر ساخت داده/ زیر ساخت های اطلاعاتی و محتوایی/ شبکه (ساختار، معماری و پیکربندی، عملیات و اجزاء، منابع و تجهیزات)/ زیر ساخت های نرم افزاری و پردازشی/ زیر ساخت های کاربردی و خدماتی/ زیر ساخت های رایانشی/ زیر ساخت های پایه/ زیرساخت های ذخیره و پشتیبان گیری
۲	**محتوا**	داده ها و اطلاعات حساس مراکز داده – اطلاعات کنترل و پایش در دیسپچینگ ها – اطلاعات موجود در سامانه های بانکداری الکترونیکی، سامانه های حوزه سلامت، سامانه های ارتباطی و حمل و نقل، سامانه های خدمات دولت الکترونیک، سامانه های خدمات حقوقی و قضایی و ....
۳	**خدمات**	نرم افزارهای پردازشی و برنامه های کاربردی، خدمات شبکه محوری، نرم افزارهای پایه
۴	**کاربر**	نیروی انسانی دارای دسترسی به اطلاعات حساس در مراکز داده، دسترسی به ساختار دیسپچینگ های ملی، افراد دارای دسترسی به سامانه های بانکداری الکترونیکی، سامانه های ناوبری، ارتباطی، کنترلی حوزه حمل و نقل، سامانه های پرونده الکترونیک سلامت، خدمات دولت الکترونیک،

		سامانه های خدمات حقوقی و قضایی و ....

رزم سایبری

در اسناد جهانی، عملیات رزم سایبری بکارگیری قابلیت های سایبری در راستای رسیدن به اهداف در/ از طریق فضای سایبری می باشد(وزارت دفاع آمریکا، ۲۰۱۸: ۵۸). عملیات فضای سایبری از دفاعی تا هجومی متفاوت است. در دستورالعمل اجرای عملیات سایبری ارتش آمریکا آماده سازی محیط عملیات سایبری، شامل فعالیت‌های توانمندساز غیر اطلاعاتی است که برای برنامه‌ریزی و آمادگی عملیات‌های نظامی انجام می‌شود. این پدیده شامل شناسایی داده، نرم‌افزار و پیکربندی شبکه یا ساختارهای فیزیکی است که به شبکه متصل بوده و یا به آن مربوط هستند و هدف، شناسایی آسیب پذیری‌های سیستم می‌باشد. آماده‌سازی محیط عملیات‌سایبری، به نیروهای آموزش دیده استانداردی نیاز دارد که از به خطر افتادن عملیات جمع‌آوری اطلاعات نظامی مربوطه جلوگیری می‌کند(اف ام ۱۲-۳، ۲۰۱۷: ۹-۱). حملات سایبری، عبارت اند از، بهره برداری عملیاتی مخرب از فضای سایبر با قابلیت‌های؛ الف) دسترسی غیر مجاز به اطلاعات حیاتی ذخیره شده یا منتقل شده ب) تخریب، اصلاح یا جایگزینی نرم افزارهای پردازشی مورد نیاز پ) محدود کردن دسترسی به عوامل کاهش دهنده پیامد حملات ذکر شده است(یوم و دیگران[1] ۲۰۱۵: ۲۵). حمله سایبری از نظر وزارت دفاع آمریکا (۲۰۱۹) عبارت است از: تلاش برای آسیب رسانی، تخریب، مختل ساختن، غیر فعال سازی، به دست آوردن دسترسی غیر مجاز به رایانه؛ سامانه رایانه ای، محیط محاسباتی، زیر ساخت محاسباتی، شبکه ارتباطی الکترونیکی از طریق فضای سایبری به منظور ازبین بردن جامعیت داده یا سرقت اطلاعات کنترل شده می باشد.

منابع توانمند ساز رزم سایبری

منابع و توانمند سازها مهمترین عوامل برای ارزیابی آمادگی رزم سایبری در سطح ملی و سـازمانی

[1].Youm et al

محسوب می‌گردد. که بدون آن ها ارزیابی آمادگی رزم سایبری معنا و مفهوم پیدا نمی کند. ونبلز[1] در مقاله‌ای تحت عنوان « مدلی برای مشخص کردن قدرت سایبری» قابلیت های سایبری را به شرح زیر بیان می کند (ونبلز،۲۰۱۵)

جدول۳ : قابلیت های سایبری(ونبلز،۲۰۱۵)

ردیف	قابلیت های سایبری
۱	مشارکت فعال و نفوذ در حوزه سایبری با استفاده از پروژه قدرت نرم
۲	اقدامات آفندی هدفمند برای دستیابی به اهداف خاص
۳	تاب آوری زیر ساخت های سایبری
۴	حفظ آگاهی وضعیتی جامع
۵	منابعی برای اقدامات تلافی جویانه
۶	پیش بینی مؤثر جذب، انطباق پذیری و بازیابی
۷	مهارت های فنی

طرح ریزی عملیات سایبری

طرح ریزی عملیات سایبری نسبت به عملیات نظامی، دارای پیچیدگی‌ها و حساسیت‌های خاصی است. عملیات‌سایبری می‌تواند در محدوده جغرافیایی و زمان مشخصی به صورت مخفیانه و بدون اطلاع رقیب با جزئیات دقیق و فنی، توسط عامل‌های انسانی و نرم‌افزاری با سطح خبرگی مشخص انجام گیرد؛ نتیجه عملیات سایبری می تواند تاثیرات مستقیم و غیرمستقیمی در هدف و سایر مؤلفه های مرتبط با آن هدف ایجاد نماید(آلن،[2]۲۰۱۷). به عنوان نمونه، در حمله سایبری به یک بانک، علاوه بر ایجاد حمله منع سرویس و وضرر مالی، می تواند باعث گسترش حمله مورد نظر به سایر سازمان ارگان های مرتبط به بانک مورد نظر شود یا در حمله سایبری به نیروگاه، بسیار مهم است که وسعت، نوع عملیات و میزان دستکاری مشخص و قابل کنترل است؛ درغیر این صورت، تبعات سیاسی، اقتصادی، اجتماعی و حقوقی برای گروه مجری و حامیان آن خواهد داشت؛ بنابراین،

[1] Adrian venables

[2] .P. D. Allen

بسیار مهم است که متناسب با نوع مأموریت، در انتخاب فرد به شرایط ویژگی هایی مثل تخصص، فکر، قوه تخیل، روحیه و تعامل و فعالیت های گروهی توجه ویژه ای شود تا درصد موفقیت عملیات بالا رفته و مجریان بتوانند به نحوه مطلوب، مطابق با شرح وظایف مأموریت، انجام وظیفه نمایند. برای طرح ریزی و انجام یک عملیات سایبری، بر اساس نوع و شرایط هدف، مجموعه مأموریت و اقداماتی تعریف می گردد. برخی از این مأموریتها تخصصی و برخی عمومی حوزه فضای سایبری هستند. به عنوان مثال، برای رصد و جمع آوری اطلاعات از منابع آشکار، عموماً افراد یک گروه می توانند این اقدام را انجام دهند در صورتی‌که استفاده و به کارگیری از یک نرم افزار خاص و یا یک فن منحصر به فرد برای انجام یک مأموریت ویژه، توسط یک فرد مشخص صورت می گیرد و نمی توان این مأموریت را به دیگری واگذار کرد. در جدول۴ برخی از مأموریت های عمومی یک عملیات سایبری، شرح داده شده است که فرمانده عملیات سایبری متناسب با مأموریت های بیان شده، طرح ریزی عملیات نموده و افراد را متناسب با تخصص و نوع مأموریت و سایر نیازمندی های عملیات به کارگیری می نماید.

جدول۴: فرآیند طرح ریزی حملات سایبری و سلاح های مربوطه

ردیف	عنوان کلی مرحله	عنوان زیر مرحله ها	سلاح های سایبری
۱	شناسایی مواضع	شناسایی سیستم	Scanner,Nessus,N_stealth
۲	هجوم اولیه	دسترسی	Sniffer,keylogger, passcracker
		تخریب	ویروس و کرم
۳	تثبیت مواضع	محو ردپاها	Rootkit
		نصب دریچه	اسب تروا
۴	برنامه ریزی بعدی	سرقت یا تخریب اطلاعات	
		سایر فعالیت های غیرمجاز	
		حمله به اهداف ثانویه	

اتخاذ رویکرد تهاجمی ایالات متحده آمریکا به فضای سایبر

ژنرال پاول ناکاسون[1]فرمانده سایبرکام در مقاله‌ای با عنوان «یک نیروی سایبری برای عملیات مداوم» ضمن بیان تاریخچه و نمونه هایی از حملات سایبری به این کشور از جمله؛ حملات انکار سرویس علیه بخش مالی(۲۰۱۳-۲۰۱۲)، حمله به کازینوSands (۲۰۱۴)، حمله کره شمالی به Sony Pictures Entertainment (۲۰۱۴)، اختلال چین درGitHub (۲۰۱۵) و سرقت داده‌های مربوط به امنیت از دفتر مدیریت پرسنل(۲۰۱۵) » اذعان می کند که: فعالیت‌های مخرب سایبری در طول زمان می‌توانند به منزله تهدید امنیت ملی، منابع قدرت ملی یک کشور را تهدید و از بین ببرند. از این‌رو راهبرد واکنشی سایبری، در واقع به مفهوم نگه داشتن نیروهای سایبری، در معرض درگیری‌های مداوم و یا واکنش پس از وقوع حملات سایبری به کشور آمریکا است؛ که این راهبرد به معنی واگذاری ابتکار عمل در فضای سایبر به دشمنانی است که مایل به فعالیت مداوم علیه کشور در فضای سایبری برای دستیابی به آثار راهبردی هستند. بنابراین نتیجه گیری و پیشنهاد می‌دهد که فرماندهی سایبری نیاز به اتخاذ یک راهبرد جدید تهاجمی دارد(ناکاسون،۲۰۱۹).[2]به همین دلیل و در راستای خوی استکباری کشور ایالات متحده آمریکا، در راهبرد سایبری ۲۰۱۸ رویکرد ایالات متحده در قلمروی سایبری، تهاجمی‌تر از گذشته هدف گذاری، سازماندهی و انتشار داده شد. در این سند پس از ارائه راهبرد برای امنیت سایبری شبکه های فدرال و حفاظت از زیر ساخت های حیاتی، در ادامه اقدامات سایبری در راستای اجرای راهبردهای سایبری نظامی را به شرح زیر بیان می کند:

۱) ساخت و حفظ نیروها و توانایی های آماده برای انجام عملیات فضای سایبری

۲) دفاع از شبکه اطلاعات، اطمینان داده‌های وزارت دفاع امریکا و کاهش خطرات ماموریت‌های وزارت دفاع امریکا

۳) آمادگی برای دفاع از کشور میزبان ایالات متحده و منافع حیاتی او با ما از حملات سایبری مخرب

۱General Paul M. Nakasone

۲ https://www.459arw.afrc.af.mil/News/Article-Display/Article/1737519/a-cyber-force-for-persistent-operations/

۴) ساخت و حفظ گزینه‌های سایبری قابل قبول و برنامه‌ریزی برای استفاده از این گزینه‌ها برای کنترل تهاجم و ایجاد محیط جنگ در تمام مراحل

۵) ساخت و حفظ اتحادها و همکاری‌های قوی بین‌المللی برای جلوگیری از تهدیدات مشترک و افزایش امنیت و ثبات بین‌المللی(سند راهبرد ملی سایبری آمریکا،۲۰۱۸).

لذا در این راستا نسبت به ایجاد و توسعه توان رزم‌سایبری در راستای تقویت و حفظ آمادگی‌نظامی خود در حوزه فضای سایبری اقداماتی را در حوزه‌های امنیتی و دفاعی انجام داده است که از اهم این اقدامات می توان به موارد زیر اشاره نمود:

۱- ارتقاء سطح سازمانی فرماندهی های سایبری در همه نیروها

۲- افزایش بودجه سایبری آمریکا در سال های اخیر

البته اهداف بودجه سایبری وزارت دفاع و برنامه‌های فرماندهی سایبری به شرح ذیل می باشند:

- ✓ افزایش قابلیت های آفندی و پدافندی در حوزه فضای سایبری
- ✓ سازماندهی مجدد و افزایش نیروهای موردنیاز، ایجاد یک نیروی مشترک برای عملیات های سایبری و ادامه پشتیبانی از سازماندهی ۱۳۳ تیم سایبری، که از سال ۲۰۱۳ آغاز شده است.
- ✓ شناسایی، کاهش و پاسخ به تهدیدات در فضای سایبری
- ✓ امن سازی شبکه های اطلاعاتی و داده های وزارت دفاع و آمادگی دفاع در برابر حملات
- ✓ انجام عملیات های سایبری آفندی جهت پشتیبانی از فرماندهان جنگی و عملیات های نظامی که باعث فراهم نمودن بازدارندگی و پاسخ به تهدیدات برای مدیران و فرماندهان می گردد.
- ✓ توسعه اختیارات سایبری جهت کنترل جنگ های سایبری
- ✓ ایجاد هم پیمانان بین‌المللی جهت کاهش تهدیدات سایبری عمومی مشترک در این راستا. در بودجه سال ۲۰۱۷ ، مبلغ ۳,۴ بیلیون دلار جهت ایجاد اطمینان برای همپیمانان ناتو و اروپایی اختصاص داده است.
- ✓ سرمایه گذاری در نوآوری روش های پیاده سازی یک محیط مجازی برای عملیات تیم های سایبری و تمرین آنها جهت ورزیدگی در برابر طیف وسیع تهدیدات و تجهیز آنها به ابزارها و پلت فرم های لازم

✓ پشتیبانی از تحقیقات جهت توسعه ابزارهای مورد نیاز نیروهای سایبری در ماموریت ها (هنری[1]،۲۰۱۷)

آمادگی رزم

آمادگی رزم یا آمادگی نظامی، شامل تدابیر بازدارنده‌ای می باشد که قبل از وقوع جنگ و درگیری در نظر گرفته می‌شود. اخذ این تدابیر، به علت وقوع جنگ‌های پی در پی، از دیر باز مورد توجه کشورها بوده است. آمادگی رزمی به منزله ایجاد قابلیت و به کیفیت درآوردن توان و استعدادهای کمی واحد نظامی برای اجرای بهینه ماموریت است و به تعبیر دیگر آمادگی رزمی: با ایجاد قابلیت و مهارت بخشی به عناصر توان نسبی، کیفیت بکارگیری آن ها را از حالت بالقوه به بالفعل مبدل می‌نماید (نوذری، ۱۳۸۹ : ۴). در سطح نیروهای مسلح جمهوری اسلامی ایران، آمادگی رزمی عبارت است از میزان قابلیت ها، توانمندی‌ها، مهارت‌ها و شایستگی‌های یک یگان نظامی در بکارگیری استعداد رزمی واگذارشده برای اجرای مأموریت می‌باشد. این آمادگی دارای ابعاد روحیه و معنویت، فرماندهی و مدیریت، آمادگی و مهارت و آمادگی سلاح و تجهیزات می‌باشد(آیین نامه آمادگی رزم، ۱۳۹۶). در ادامه به مهمترین مؤلفه‌های مؤثر در آمادگی رزم سایبری پرداخته شده است:

آمادگی نیروی انسانی

اگر چه نقش تسلیحات و تجهیزات و فنآوری های پیشرفته به عنوان یک پیشران اصلی در اقتدار در پیروزی در جنگ انکار ناپذیر است ولیکن در نظام جمهوری اسلامی قوام اصلی نیروهای مسلح بر سرمایه انسانی استوار است. وجود نیروی انسانی با انگیزه، مؤمن، شهادت طلب، باکیفیت و کارآمد به عنوان مهمترین عامل به حساب می‌آید. در جبهه های غربی و شرقی مقابل ما توجه‌ای به عامل ایمان و اعتقاد مردم نشده است. فقط به عامل روحی روانی توجه دارند که البته موثر است ولی با عامل ایمان بسیار متفاوت می‌باشد. در سال‌های اخیر ملت ایران و جبهه مقاومت معجزه ایمان را در رویارویی با کافران، تکفیری ها و ارتجاع نشان داده اند. یدالله فوق ایدیهم باور قلبی

[1] . henry jamal,

مومنین است و با اعتقاد به آن امدادهای الهی را جذب می‌کنند. خداوند در قرآن کریم می فرمایند: یا أَیُّهَا النَّبِیُّ حَرِّضِ الْمُؤْمِنِینَ عَلَی الْقِتالِ إِنْ یَکُنْ مِنْکُمْ عِشْرُونَ صابِرُونَ یَغْلِبُوا مِائَتَیْنِ (انفال ۶۵). ای پیامبر! مؤمنان را بر پیکار (با کفّار) تشویق کن، اگر بیست نفر از شما پایدار باشند، بر دویست نفر پیروز می‌شوند واگر از شما صد نفر (مقاوم) باشند، بر هزار نفر از کافران غلبه می‌یابند.

مهارت های سایبری

مهارت مهاجم در حملات سایبری عبارت است از؛ به کارگیری توانایی ها و تجربیات کارا (تکنیک ها مانند تغییر روش ها و تاکتیک ها مانند افزایش یا کاهش بات) که وضعیت خدمت رسانی مدافع را تنزل دهد. به طوریکه مهاجم ماهر باید قادر باشد اقدامات مدافع را درست درک کند و اقدام صحیح متقابل را انجام دهد(اکبری و همکاران، ۱۳۹۷). نظر به اینکه کارائی هر سازمان و اثر بخشی ماموریت های آن به طور مستقیم به کارایی و کارآمدی نیروی انسانی آن سازمان وابسته است از این رو، موضوع مهارت به عنوان یکی از مؤلفه‌های اصلی و بسیار مؤثر در ارزیابی آمادگی رزم سایبری نیروهای مسلح که همان توجه به نیروی انسانی متخصص، دانا و توانا در حوزه سایبری است مورد توجه جدی قرار می گیرد. اهمیت این موضوع به گونه ای است که، واحد پیامدهای سایبر آمریکا تخصص های مورد نیاز برای اجرای موفقیت آمیز حملات سایبری را به شرح جدول۵ دسته بندی نموده است.

جدول۵: تخصص های لازم برای موفقیت در حملات سایبری (اسکات،۲۰۱۵، واحد پیامدهای سایبر آمریکا)

ردیف	نوع تخصص/مهارت	شرح
۱	**انتخاب هدف**	انتخاب اهداف خاص و تنوع حملاتی که مهاجم به نفع خود انجام می دهد
۲	**تخصص دسترسی**	شناسایی راه های ورود و دسترسی به اطلاعات مرتبط سامانه ها
۳	**تخصص فرآیند**	دانستن به طور دقیق ورودی اطلاعات و یا تولید اختلال در نتایج مورد نظر
۴	**تخصص برنامه نویسی**	توانمندی نوشتن کد و داده برای تولید اختلال مورد نظر

البته در خصوص نحوه سازماندهی و بکارگیری نیروی انسانی در اجرای موفقیت آمیز عملیات سایبری از حیث بعد شناختی و ادراکی نیروی انسانی، بایستی به این نکته بسیار مهم و اساسی

توجه نمود که: هر کسی قادر به انجام کار در این محیط نخواهد بود. تربیت و آموزش در بالاترین و گسترده ترین سطح ممکن باید انجام پذیرد اما تمرکز اصلی می بایست بر تشکیل تیم مرکزی متشکل از متخصصین بسیار کارآمد و ویژه باشد (لینتون ولز، ۲۰۱۸).

آمادگی فناوری و تسلیحات سایبری بومی

در ادبیات دانشگاهی و نظامی، تعاریف مختلفی برای سلاح سایبری بیان شده‌است، تعریف مشترک روسیه و آمریکا از این واژه را « نرم افزار، سفت‌افزار(فِرم‌ویر)[1] یا سخت‌افزار طراحی‌شده یا اعمال‌شده برای ایجاد آسیب از طریق دامنه سایبری» بیان می‌کند(مؤسسه شرق- غرب،[2]۲۰۱۴). راهنمای تالین(۲۰۱۷)، سلاح سایبری را « ابزار سایبری جنگ » معرفی می‌کند که با طراحی یا استفاده می‌تواند باعث آسیب رساندن به افراد یا اشیاء گردد. سلاح‌های سایبری بر اساس ماموریت مورد انتظار به انواع سلاح‌های شناسایی، وارسی، نفوذ ، هجوم و تسلیحات منع خدمات و سرویس تقسیم می‌شوند (بابک و همکاران،۱۳۹۶).

آگاهی وضعیتی سایبری

فهم و درک اینکه چه چیزی اتفاق افتاده و یا در حال رخ دادن است و یا اینکه ممکن است در آینده نزدیک اتفاق بیفتد را آگاهی وضعیتی گویند، به طوری‌که این درک، از فهم عناصری (موضوع مورد توجه) از محیط حاصل می‌شود که به یکدیگر مربوط می‌شوند. مباحثی همچون نحوه کسب آگاهی و استنتاج آن و عوامل تأثیرگذار در درک (بهتر یا بدتر) انسانی یا ماشینی، مورد نظر پژوهشگران این حوزه است. در تمامی حوزه های عملیاتی تلاش می شود تا وضعیت ها معین گردد، سپس با استفاده از قرائن و شواهد و سایر روش‌های استنتاجی تشخیص داده می‌شود که کدام وضعیت در حال رخ دادن است یا در آینده‌ای نزدیک ممکن است.

---

[1] Firmware

برنامه نرم‌افزاری سطح پایین که توسط سازنده در حافظه دائمی سخت‌افزار تعبیه می‌شود و حاوی داده‌ها و کدهای پایه‌ای است که استفاده و کنترل سخت‌افزار را ممکن می‌سازد. سازنده بعضاً با بسته‌های جدید، امکان به‌روز رسانی فریم‌ویر را برای اضافه نمودن امکانات جدید فراهم می‌کند.

[2] East-West Institute

شاخص های کسب آگاهی وضعیتی سایبری عبارتند از: پایش سایبری، شناسایی قابلیت های پدافند سایبری دشمن، هشدار دهی و تقسیم فضای سایبری می باشند (نصرت آبادی،۱۳۹۸). هدف نهایی ارائهٔ آگاهی وضعیتی سایبری، تصمیم گیری درست و به موقع برای طرح ریزی حملات سایبری می‌باشد.

مدل مفهومی(ابعاد و مؤلفه های) آمادگی رزم سایبری

همان گونه که در ادبیات تحقیق اشاره شد، فضای سایبر مشتمل بر سه بعد فیزیکی، اطلاعاتی و شناختی می باشد. در ادامه بیان شد که اجزاء تشکیل دهنده این فضا قابل تفکیک به اجزای زیر ساختی، خدماتی، محتوی و کاربران این فضا می باشد. از طرفی سه اصل مهم برای حفظ، حراست، پایداری و صحت اطلاعات وجود دارد که در حوزه سایبری، حفاظت و مراقبت از این سه اصل، هدف اصلی امنیت سایبری است و هرگونه خدشه به این سه پارامتر به مثابه حمله و رزم سایبری تلقی می گردد. با توجه به هدف تحقیق، به منظور شناسایی ابعاد رزم سایبری و با عنایت به نظر حکمایی همچون مرحوم شاه‌آبادی که به منظور درک و شناخت درست پدیده‌ها، بایستی موضوع یا پدیده مورد نظر را از منظر(فاعل موضوع، بستر، فعل و روش) مورد بررسی قرار داد(شهیر، ۱۳۹۶). لذا عوامل مؤثر بر حوزه آمادگی رزم سایبری پس از جمع بندی نظر خبرگان، مطابق جدول ۶ قابل دسته‌بندی می‌باشند.

جدول۶: شناخت ابعاد رزم سایبری (محقق ساخته)

شناخت ابعاد و مؤلفه های رزم سایبری	بستر	سطوح رزم سایبری مشتمل بر رزم فیزیکی/اطلاعاتی و شناختی سایبری
	فاعل	بازیگران اجرای رزم سایبری اعم از نیروی انسانی(با انگیزه ، ولایی و ماهر) ، تسلیحات، فناوری های اجتماعی سایبری
	روش	اقدامات عملکردی رزم سایبری مبتنی بر مفاهیم عملیاتی شامل دکترین سایبری، آگهی وضعیتی سایبری، سناریو اقدام، طرح ریزی و اجرا، ارزیابی و تحلیل مستمر
	فعل	سبک فرماندهی، مدیریت و هدایت سایبری شامل مشروعیت بخشی برای رزم سایبری، سیاستگذاری و برنامه ریزی، سازماندهی و هماهنگی

نظر به موارد فوق تعریف عملیاتی از مفهوم آمادگی رزم سایبری؛ میزان آماده بودن: بستر رزم، بازیگران عملیاتی، آماده بودن الزامات روشی و نحوه اعمال فرماندهی و هدایت سایبری برای اجرای رزم در فضای سایبر می‌باشد.

روش شناسی تحقیق

این پژوهش، از نظر هدف کاربردی و از حیث گردآوری داده ها، توصیفی- پیمایشی محسوب می‌شود. جهت دستیابی به هدف پژوهش از هر دو روش گردآوری اطلاعات، یعنی روش کتابخانه‌ای(فیش برداری) و روش‌های میدانی(مصاحبه ومشاهده) بهره گیری شده است. جامعه آماری مورد نظر در این تحقیق متناسب با روش مورد استفاده در گردآوری اطلاعات نخست شامل: آثار مکتوب و اسناد و مدارک بالادستی و مرتبط با موضوع تحقیق و سپس شامل خبرگانی می باشد که مسلط به مسائل راهبردی فضای سایبر بوده و در حوزه رزم و آمادگی رزم سایبری صاحب نظر باشند. بنابراین تعداد آنان بسیار محدود بوده لذا با بهره گیری از روش هدفمند گلوله برفی، تعداد آنها احصاء شده است. با این روش ابتدا در بخش کیفی به منظور تولید ادبیات در خصوص الگوی مفهومی آمادگی رزم‌سایبری در قالب مصاحبه عمیق، تعداد ده نفر از اساتید هیئت علمی دانشگاه‌ها و پژوهشکده‌های مرتبط با سایبر، مدیران و کارشناسان حرفه‌ای در سطوح ستادی و عملیاتی در رابطه با موضوع این تحقیق شناسایی شدند. همچنین در بخش‌کمی تعداد ۳۰ نفر از جامعه آماری مورد اشاره برای نظرخواهی و پاسخ به پرسش‌نامه محقق ساخته انتخاب گردیدند. در اثبات‌روایی(اعتبار ابزارهای این تحقیق)، از روش اعتبار محتوا استفاده شده است. در این‌روش، فرم‌های طراحی شده برای مصاحبه و پرسش نامه به وسیله‌ی تعدادی از خبرگان در رابطه با موضوع تحقیق مورد ارزیابی و پس از اعمال اصلاحات لازم مورد تائید قرار گرفت. برای محاسبه پایایی (قابلیت اعتماد) پرسش‌نامه، از فرمول آلفای کرونباخ در نرم افزار SPSS استفاده شد که آلفای محاسبه شده برای دو بخش ابعاد، و اولویت‌بندی در نظر گرفته شده در پرسش نامه به ترتیب ۰/۸۱ و ۰/۸۹ می‌باشد که با در

نظـرگرفتـن حداقـل ضریب ۰/۵ بـرای تأییـد پایایی ابـزار تحقیق، نشانگر پایـایی خـوب و قابل قبولی است.

یافته ها و تجزیه و تحلیل داده‌ها

شیوه تجزیه وتحلیل داده در این تحقیق استفاده از رویکردهای کیفـی و کمـی اسـت. در رویکـرد کیفی پس از مطالعه دقیق ادبیات تحقیق و انجام مصاحبه با خبرگـان، بـا اسـتفاده از روش تحلیـل محتوا، تحلیل و کدگذاری شدند. واحد تحلیل محتوا در این پژوهش، مضمون بود. به ایـن ترتیـب یک پاراگراف یا جمله یا بخشی از آن استفاده شد و یک کد به صورت عددی یا به عنوان یک متن اختصاص داده شد.پس از کدگذاری، کدگذاری محوری انجام شد. دراین مرحله، همـان کـدها بـه صورت مفهومی طبقه بندی شدند. پس از طبقه بندی، ابعاد و مؤلفه های مؤثر در الگـوی مفهـومی آمادگی رزم سایبری استخراج و مطابق جدول۷ در چهار بعد بستر رزم سایبری، بازیگران عملیاتی، روش رزم و نحوه عملکرد فرماندهی و مدیریت سایبری دسته بندی شده است.

جدول۷: ابعاد و مؤلفه های الگوی مفهومی آمادگی رزم سایبری

مفهوم	ابعاد	مؤلفه ها
آمادگی رزم سایبری	بستر رزم سایبری	**فیزیکی**
		اطلاعاتی
		شناختی
	بازیگران عملیاتی	**نیروی سایبری سازمان یافته ماهر**
		تسلیحات سایبری بومی فعال و بالقوه
		فناوری های اجتماعی بومی
	روش رزم	دکترین سایبری
		آگهی وضعیتی سایبری
		تدوین سناریو
		طرح ریزی عملیاتی
		ارزیابی و تحلیل مستمر

		پشتیبانی فنی و تخصصی
	سبک فرماندهی و مدیریت سایبری	مشروعیت بخشی پاسخ به حملات سایبری
		جدیت در پاسخ به حمله سایبری
		سیاستگذاری و برنامه ریزی
		سازماندهی
		هماهنگی

جهت تایید نرمال بودن داده‌ها، از آزمون کلموگوروف - اسمیرنوف استفاده شد. فرض صفر در این آزمون این است که بین فراوانی مشاهده شده و مورد انتظار تفاوتی وجود ندارد و به عبارت دیگر، توزیع جامعه نرمال است. اگر asymp. sig. (2-tailed) سطح خطا بیشتر از ۰,۰۵ باشد، دلیلی برای رد فرضیه صفر وجود ندارد و می‌توان گفت داده‌ها دارای توزیع نرمال می‌باشند. و اگر کمتر از مقدار مورد نظر باشد، با عدم توزیع نظرات مواجه هستیم. براساس نتایج به‌دست آمده از این آزمون، داده‌ها دارای توزیع غیر نرمال می‌باشند و برای آزمون فرضیه های دیگر پژوهش، باید از روش های ناپارامتریک آماری استفاده کرد. با مشخص شدن توزیع غیرنرمال داده ها، برای رتبه بندی و تعیین میزان اهمیت ابعاد و معیارهای پیشنهادی، از آزمون فریدمن استفاده شد. آزمون فریدمن، از جمله آزمون های معروف ناپارامتریک است که برای رتبه بندی و مقایسه گروه های مختلف در صورتی که نوعی وابستگی بین اعضای گروه های مختلف وجود داشته باشد، به کار می رود. فرض صفر و فرض مقابل در این آزمون، به این صورت نوشته می شود: فرض صفر- میانگین رتبه های چند عامل با هم یکسان است. فرض مخالف- حداقل یک جفت از عوامل، میانگین رتبه یکسانی ندارند.

طبق نتایج به دست آمده در جدول ۸ و با توجه به فرض های آماری و مقدار آماره آزمون ها، همان طورکه انتظار می رفت، خبرگان اهمیت یکسانی برای ابعاد و معیارهای مؤثر در انتخاب و اولویت بندی آمادگی رزم سایبری قائل نیستند. از نظر خبرگان، نخست بعد بستر رزم سایبری و سپس ابعاد بازیگران رزم سایبری، روش رزم و عملکرد سبک فرماندهی و مدیریت در اولویت قرار دارند.

جدول۸: نتایج آزمون کلموگوروف- اسمیرنوف (نحوه ی توزیع داده ها) و آزمون فریدمن

ابعاد	مقدار آماره آزمون کلموگوروف–اسمیرنوف Sig (ابعاد)	اختصار	مقدار آماره آزمون کلموگوروف–اسمیرنوف Sig (اولویت بندی)	مقدار آماره آزمون فریدمن (ابعاد)	مقدار آماره آزمون فریدمن (اولویت بندی)	رتبه (ابعاد)	رتبه (اولویت بندی)
بستر رزم سایبری	۰/۰۰۱	B1	۰/۰۳	۶/۱۳	۲۳/۳۵	۱	۹
		B2	۰/۰۰		۲۶/۴۲		۱
		B3	۰/۰۲		۲۱/۷۰		۱۲
بازیگران عملیاتی	۰/۰۰۰	A1	۰/۰۰	۶/۰۸	۲۵/۵۳	۲	۲
		A2	۰/۰۲		۲۵/۵۲		۳
		A3	۰/۰۲		۲۰/۹۳		۱۳
روش رزم سایبری	۰/۰۰۱	M1	۰/۰۴	۵/۶۲	۲۱/۸۵	۳	۱۱
		M2	۰/۰۳		۲۵/۱۰		۴
		M3	۰/۰۰		۲۴/۶۸		۵
		M4	۰/۰۲		۲۴/۳۲		۶
		M5	۰/۰۱		۲۳/۹۳		۷
		M6	۰/۰۲		۲۳/۵۲		۸
عملکرد فرماندهی و مدیریت سایبری	۰/۰۰۰	P1	۰/۰۰	۵/۴۷	۲۳/۱۰	۴	۱۰
		P2	۰/۰۱		۲۰/۳۸		۱۴
		P3	۰/۰۱		۱۹/۳۲		۱۵
		P4	۰/۰۱		۱۹/۰۸		۱۶
		P5	۰/۰۰		۱۸/۹۰		۱۷

نتیجه گیری و پیشنهاد

الف) نتیجه گیری: مطلب مهم در هر پژوهش‌علمی این است که، کار تحقیقی باید همیشه با

اجتهاد و اظهارنظر توام باشد و محقق در پایان کار و بر اساس مطالعات انجام‌شده بـه طـور قـاطع نظر خود را درباره موضوع اعمال دارد تا به گسترش دامنه معرفتی علم و یافته های موجود کمـک کند(حافظ نیا،۱۳۸۱: ۲۲۱). علیرغم به کارگیری زیاد عبـارت آمـادگی‌رزمـی، شـاهد پراکنـدگی و تفاوت میان تعریف‌ها و مضمون های به کار گرفته شده برای این عبارت هستیم. **مفهوم آمـادگی رزمی، از یک نظر به معنی آمادگی نیروها در صحنه جنگ و از منظر دیگر به معنـای توانـایی اتمام مأموریت در جنگ محسوب می‌شود. از طرفی کاربرد روز افزون ایـن عبـارت چـه در ادبیات دانشگاهی و چه در محیط های کاربردی و عملیاتی، نیاز مفهوم پردازی دقیق و انجـام مطالعات علمی و عملی درباره چگونگی و فرآیندهای تحقق آن را ایجاد کرده است. بنـابراین باتوجه به خلاءهای موجود ارائه تعریفی جامع برای این موضوع، بسیار لازم به نظر می رسـد تا از آن طریق بتوان مطالعات آینده در این حوزه را هدایت کرد. برای این منظور محقق، برای پاسخ به سؤالات این تحقیق و دستیابی به الگوی مفهومی آمادگی رزم سایبری، ابتدا داده‌هـای اولیه شامل مقالات، کتب و اسناد بالادستی پیرامون موضوع و همچنین آراء و نظرات خبرگـان و متخصصان در موضوع، گردآوری شد و در پایان الگوی مفهومی آمادگی رزم سایبری شامل ۴ بعد:بستر رزم‌سایبری، بازیگران عملیاتی، روش رزم‌سایبری و نحوه فرمانـدهی، مـدیریت و هدایت سایبری در قالب ۱۷ مؤلفه، تدوین و ارائه شـده اسـت. جهـت اعتبارسـنجی الگـو و بررسی معناداری آن به جامعه آماری ارجاع شده است. طبق نتایج به دست آمده در جـدول ۸ و با توجه به فرض های آماری** و مقدار آمـاره آزمون هـا، همان طـور کـه انتظـار می رفت، خبـرگان اهمیت یکسـانی بـرای ابعـاد و معیارهـای مؤثـر در انتخـاب و**اولویـت بنـدی آمادگی رزم‌سایبری قائل نیستند. از نظر خبرگان، نخست بعد بستر رزم‌سایبری و سـپس ابعـاد بازیگران رزم‌سایبری، روش رزم و عملکرد سبک فرماندهی، مـدیریت و هـدایت سـایبری در اولویت قرار دارند.**

ب) پیشنهادها:

پیشنهاد های اجرایی

(۱) با عنایت به کاربردی بودن این پژوهش، پیشنهاد می‌گردد رده های نیروهای مسلح ج.ا.ا با توجه به مدل مفهومی مذکور، چگونگی فرآیندهای تثبیت و ارتقاء میزان آمادگی رزم سایبری رده های خود را ایجاد نمایند.

(۲) مدل پیشنهادی این تحقیق، سرلوحه برنامه ریزی ها، ارزیابی ها و نظارت های راهبردی فرماندهان و ستاد های بالا دستی در سطح نیروهای مسلح ج.ا.ا قرارگیرد.

پیشنهاد برای پژوهش های آتی

(۱) با توجه به تائید الگوی مفهومی، پیشنهاد می شود در تحقیقات بعدی مدل عملیاتی این الگو، با تدوین شاخص ها و سنجه های خرد طراحی گردد.

(۲) در تحقیقات بعدی با استفاده از این الگو، کاربست های ارتقاء میزان آمادگی رزم سایبری نیروهای مسلح ج.ا.ا تدوین گردد.

(۳) نظام ارزیابی آمادگی رزم سایبری نیروهای مسلح با استفاده از الگوی مفهومی مذکور طراحی گردد.

فهرست منابع و مآخذ

الف. فارسی

- اکبری، حمید و همکاران(۱۳۹۸). آگهی وضعیتی حملات منع خدمات توزیع شده بـر اسـاس پیش بینی صحنه نبرد، ***نشریه علمی پدافند الکترونیکی و سایبری***، شماره ۱ صص ۹۴-۷۷
- تقی پور، رضا و همکاران (۱۳۹۸). الگوی راهبـردی حفاظـت سـایبری از زیـر سـاخت هـای اطلاعاتی حیاتی ج.ا.ا، ***فصلنامه علمی امنیت ملی***، سال نهم، شماره ۳۴، صص ۴۸-۷
- ***سند راهبردی پدافند سایبری کشور*** (۱۳۹۴). سازمان پدافند غیرعامل کشور
- شهیر، احسان و همکاران (۱۳۹۶). ***طراحی الگوی راهبردی بـومی امنیـت فضـای مجـازی کشور***، رساله دکتری، دانشگاه عالی دفاع ملی، دانشکده امنیت ملی
- نای، جوزف، (۱۳۹۰). ***آینده قدرت***، ترجمه صحرایی، رضا مراد ،حروفیه ،تهران
- نصرت آبادی، جمشید و همکاران،(۱۳۹۸). ***الگوی ارزیابی قدرت سایبری نیروهـای مسـلح جمهوری اسلامی ایران***، رساله دکتری، دانشگاه عالی دفاع ملّی، دانشکده امنیت ملی
- نوذری، فضل الله(۱۳۸۹). ***مفاهیم آمادگی رزمی و اصول جنگ***، چاپ اول، تهران، دانشکده و پژوهشکده علوم دفاعی
- هلیلی، خداداد و همکاران(۱۳۹۷). ***ارائه الگوی راهبردی ارتقاء قدرت سایبری ج.ا.ا در تراز جهانی***، رساله دکتری، دانشگاه عالی دفاع ملی، دانشکده امنیت ملی

ب. انگلیسی

- Adrian Venables, siraj Ahmed sheikh andjames shuttleworth (2015). A model for characterizing cyber power 9th ***international conference on critical infrastructure protection*** (ICCIP).
- Andress ،J. ،& Winterfeld ،S. (2013). Cyber warfare: techniques،3. tactics and tools for security practitioners: ***Elsevier.***
- FFIEC, (2015), FFIEC ***Cybersecurity Assessment Tool***. Appendix C: Glossary, pp 1-38.
- Euisun Paik, Heung Youl Youm, (2015), " ***Knowledge Sharing Series***

Cybersecurity", APCICT Publication, PP 1-108

- Ugur Akyazi, (2014), ***"Possible Scenarios and Maneuvers for Cyber Operational Area",*** 13th European Conference on Cyber Warfare and Security - Cryptome, PP15-21.
- P. D. Allen, "***Information operations planning***," Artech House, 2017.
- Training and Doctrine Command (TRADOC) Pamphlet 525-7-8, ***"The U.S Army Concept Capability Plan for Cyberspace Operation*** (CyberOps)" 2016-2028, February 2010
- Eastwest Institute and the Information Security Institute of Moscow State University, "***Russia-U.S. Bilateral on cybersecurity - critical terminology foundations***", Issue I, April 2011
- Carlisle Barracks, ***"U.S Army war college guide to national security issues",*** Volume I: Theory of war and strategy , 5th Edition, June 2012
- NATO Cooperative Cyber Defence Centre of Excellence, ***"National Cyber Security Framework Manual",*** 2012, PP 8-19
- UK Cabinet Office, "***The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world",*** November 2011
- The White House, "***Cyberspace Policy Review: Assuring a Trusted and Ressilient Information and Communications Infrastructure***", May 2009
- oint Chiefs of Staff, ***"Joint Publication 3-12: Cyberspace Operations",*** 2013
- David Clark, ***" Characterizing,cyberspace:,past,,present,and,future"***, 2010